International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

The impact of cyber-attacks on Nigerian banks and strategies for mitigation

Chinonso Joseph Okonkwo [1,*] and Obumneme Solomon Okonkwor [2]

[1] *Computer Science Department, Chukwuemeka Odumegwu Ojukwu University.*
[2] *Banking and Finance Department, Federal Polythenic, Oko.*

International Journal of Science and Research Archive, 2025, 15(02), 758-761

Publication history: Received on 03 April 2025; revised on 10 May 2025; accepted on 12 May 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1419

Abstract

The Nigerian banking sector has witnessed a substantial surge in cyber-attacks, causing notable financial losses, operational disruptions, and reputational damage. As banks adopt digital platforms to enhance service delivery and financial inclusion, they have increasingly become targets of sophisticated cyber threats such as phishing, malware, business email compromise, and insider fraud. Drawing on authoritative data from the Financial Institutions Training Centre (FITC), Nigeria Inter-Bank Settlement System (NIBSS), and the Central Bank of Nigeria (CBN), this study critically examines the nature and consequences of cyber-attacks on Nigerian banks. It further evaluates regulatory interventions and institutional strategies aimed at mitigating these threats. Findings underscore the urgency for investment in robust cybersecurity infrastructure, regulatory compliance, and multi-stakeholder collaboration to ensure the integrity and resilience of the Nigerian financial ecosystem.

Keywords: Cyber-Security; Nigerian Banks; Fraud; Phishing; Regulatory Compliance; Digital Banking; Insider Threats; Cybercrime Legislation

1. Introduction

The integration of digital technologies in banking has redefined financial services in Nigeria, facilitating ease of access, transaction speed, and financial inclusion. Digital banking channels such as mobile apps, online banking platforms, USSD codes, and ATM services have seen exponential growth. However, this digital evolution comes with increased vulnerability to cyber threats. According to the Nigeria Inter-Bank Settlement System (NIBSS), fraud incidents have spiked in parallel with the growth of digital transactions.

In the second quarter of 2024 alone, Nigerian banks reported a staggering ₦42.6 billion in losses due to cyber fraud, surpassing the total fraud-related losses recorded for the entire year of 2023 (Nairametrics, 2024). This trend reflects a broader shift in the threat landscape, where attackers are becoming more organized and technologically advanced.

2. Literature review

Cyber-security in banking is a global concern, with developing countries like Nigeria facing unique challenges due to limited resources and regulatory enforcement gaps. According to Oludele and Awotunde (2023), the prevalence of cybercrime in Nigeria is exacerbated by weak institutional frameworks, poor public awareness, and insufficient collaboration between stakeholders. Udechukwu et al. (2022) emphasize the need for advanced threat detection tools and the implementation of the ISO/IEC 27001 standard in Nigerian banks.

Furthermore, research by Adebayo et al. (2021) indicates that phishing, social engineering, and malware attacks are the most prevalent forms of cyber threats affecting Nigerian financial institutions. The Central Bank of Nigeria (CBN) has

* Corresponding author: Chinonso Joseph Okonkwo.

responded by rolling out a Risk-Based Cybersecurity Framework that mandates a structured governance and compliance model for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs).

3. Methodology

This study adopts a qualitative research design, drawing on secondary data from published reports and regulatory documents. Sources include

- Quarterly fraud reports from the Financial Institutions Training Centre (FITC)
- Fraud data analytics from Nigeria Inter-Bank Settlement System (NIBSS)
- Cybersecurity circulars and frameworks from the Central Bank of Nigeria (CBN)
- Press releases and news articles from reputable media outlets such as Nairametrics and Techpoint Africa

The data was analyzed to identify patterns, common attack vectors, regulatory responses, and mitigation strategies employed by Nigerian banks.

4. Results and discussion

4.1. Nature of Cyberattacks

The most common types of cyberattacks affecting Nigerian banks include

- Phishing and Social Engineering: Fraudsters use deceptive emails and cloned websites to steal login credentials. These attacks have spiked with the rise of online banking.
- Business Email Compromise (BEC): Attackers impersonate executives to initiate fraudulent fund transfers. Nigerian banks dealing with high-value transactions are particularly vulnerable.
- Malware and Ransomware: Cybercriminals deploy malicious software to encrypt data or spy on internal networks, often demanding ransom for data restoration.
- Insider Threats: According to Techpoint Africa (2024), insider involvement in fraud rose by 23.4% in second Quarter of 2024, leading to the dismissal of 49 bank employees.

4.2. Financial and Operational Impact

Between January and September 2024, banks lost ₦53.4 billion to cyber fraud (Nairametrics, 2024). These losses translate into reduced profitability, lower investor confidence, and increased insurance premiums.

Cyberattacks also cause significant operational disruptions, including downtime of digital platforms and delayed transaction processing. This undermines customer experience and affects overall productivity.

4.3. Reputational and Regulatory Impact

Frequent cyber incidents damage public trust in the financial system. Customers affected by fraud may switch banks or avoid digital platforms altogether.

From a regulatory standpoint, failure to comply with CBN's Risk-Based Cybersecurity Framework can result in substantial penalties. The Cybercrimes (Prohibition, Prevention, etc.) Act, amended in 2024, also imposes a 0.5% cybersecurity levy on electronic transactions to fund national security initiatives (KPMG Nigeria, 2024).

4.4. Strategies for mitigation

4.4.1. Technological Advancements

Banks are advised to implement multi-layered security architecture, including:

- Multi-factor authentication (MFA)- Multi-Factor Authentication is a layered security approach requiring users to present two or more independent credentials:
  - Knowledge factor (e.g., password or PIN),
  - Possession factor (e.g., mobile device or token), and
  - Inherence factor (e.g., biometric data).

This will go a long way to reduce the risk of unauthorized access due to compromised credentials.

- Intrusion Detection Systems (IDS)- IDSs are tools that monitor networks or systems for suspicious activities or known threats
- Security Information and Event Management (SIEM) systems- SIEM systems centralize, analyze, and correlate security data from across IT environments
- AI and machine learning for anomaly detection- AI and ML technologies analyze large volumes of data to identify deviations from normal behavior, which may indicate- Insider threats,Zero-day malware,Data exfiltration.

4.4.2. Employee and Public Awareness

Institutions must conduct regular training and simulation exercises to educate staff on emerging threats. Public awareness campaigns can help reduce customer susceptibility to phishing and scam messages. This can be brought down to the public through advertorials - online and offline.

4.5. Regulatory Compliance and Auditing

Regular audits ensure compliance with CBN guidelines and international standards such as ISO/IEC 27001. Banks should also report incidents promptly to regulatory authorities.

4.5.1. Collaboration and Intelligence Sharing

The Nigerian Electronic Fraud Forum (NeFF) provides a platform for inter-bank collaboration on fraud intelligence. Joint efforts with law enforcement and telecom operators enhance threat response.

4.5.2. Incident Response Planning

Banks must develop and test incident response frameworks that include

- Rapid containment protocols
- Data backup and recovery procedures
- Communication strategies to manage public relations

5. Conclusion

The escalating rate of cyberattacks in Nigeria's banking sector highlights a pressing need for holistic cybersecurity strategies. By strengthening technological defenses, ensuring regulatory compliance, and fostering multi-sector collaboration, Nigerian banks can better protect themselves against cyber threats. Future policies must prioritize proactive measures, including the adoption of AI-driven cybersecurity tools and ongoing threat intelligence sharing, to ensure the resilience and sustainability of Nigeria's financial ecosystem.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Nairametrics. (2024, September 14). Nigerian banks lose N42.6 billion to fraud in Q2 2024. Retrieved from https://nairametrics.com/2024/09/14/breaking-nigerian-banks-lose-n42-6-billion-to-fraud-in-q2-2024-surpassing-full-year-2023-record/

[2] Techpoint Africa. (2024, November 27). Nigerian banks terminated 49 staff over fraud in Q2 2024. Retrieved from https://techpoint.africa/2024/11/27/nigerian-banks-terminated-49-staff-over-fraud-in-q2-2024/

[3] Nairametrics. (2024, November 26). Concerns as fraudsters increase attacks on banks, N115.9 billion on target in Q3 2024. Retrieved from https://nairametrics.com/2024/11/26/concerns-as-fraudsters-increase-attacks-on-banks-n115-9-billion-on-target-in-q3-2024/

[4] Digital Policy Alert. (2024, July 1). Implemented CBN Risk-Based Cybersecurity Framework. Retrieved from https://digitalpolicyalert.org/event/25171-implemented-cbn-risk-based-cybersecurity-framework-and-guidelines-for-deposit-money-banks-and-payment-service-banks-including-minimum-cybersecurity-requirements

[5] KPMG Nigeria. (2024, May). CBN Issues Guidance on the National Cybersecurity Levy. Retrieved from https://kpmg.com/ng/en/home/insights/2024/05/central-bank-issues-guidance-on-the-collection-and-remittance-of-the-national-cybersecurity-levy-by-financial-institutions.html

[6] Oludele, T. & Awotunde, J.B. (2023). Cybersecurity Challenges in Nigerian Banking Sector. Journal of African Digital Security, 5(2), 34-48.

[7] Udechukwu, P., Olayemi, T., & Eze, C. (2022). Implementing ISO/IEC 27001 in Nigerian Banks. African Journal of Fintech and Policy, 3(1), 11-23.

[8] Adebayo, R., Yusuf, S., & Bello, M. (2021). Cyber Threats and Financial Institutions: A Nigerian Perspective. International Journal of Cybersecurity Research, 6(4), 45-62.